Jelszómenedzser szoftver alkalmazása az egészségügyben

Ködmön József dr.

Debreceni Egyetem, Egészségügyi Kar, Egészségügyi Informatikai Tanszék, Nyíregyháza

Több informatikai rendszer alkalmazása esetén komoly problémát jelent a jelszavak biztonságos kezelése. Gyakran okoz nehézséget a megfelelő hosszúságú és bonyolultságú jelszavak megválasztása, illetve az erős jelszavak megjegyzése. Erre a problémára jó megoldást biztosít egy jelszómenedzser szoftver használata, amivel jelentősen növelhető az érzékeny egészségügyi adatok kezelésének biztonsága. Ez a cikk egy ilyen szoftver alkalmazásának alapvető tudnivalóit mutatja be. Tárgyalja a valóban biztonságos jelszómenedzser szoftver kiválasztását, és javasol egy konkrét alkalmazást a hatékony, biztonságos és kényelmes egészségügyi használathoz. Orv. Hetil., 2016, *157*(52), 2066–2073.

Kulcsszavak: orvosi informatika, információvédelem, jelszó

Application of password manager software in health care

When using multiple IT systems, handling of passwords in a secure manner means a potential source of problem. The most frequent issues are choosing the appropriate length and complexity, and then remembering the strong passwords. Password manager software provides a good solution for this problem, while greatly increasing the security of sensitive medical data. This article introduces a password manager software and provides basic information of the application. It also discusses how to select a really secure password manager software and suggests a practical application to efficient, safe and comfortable use for health care.

Keywords: medical computer science, information protection, password

Ködmön, J. [Application of password manager software in health care]. Orv. Hetil., 2016, *157*(52), 2066–2073.

(Beérkezett: 2016. augusztus 31.; elfogadva: 2016. október 21.)

Az informatika egészségügyi alkalmazása gyógyító tényezővé vált, ma már az egészségügy működése nem képzelhető el számítógépek és informatikai megoldások nélkül. Ez egyrészt javítja az ellátás minőségét és hatékonyságát, másrészt számos korábban nem tapasztalt problémát is felszínre hoz. Nagy tömegű érzékeny adatot kell kezelni, a korábbi – évtizedek alatt kialakult – módszerektől, szokásoktól eltérő módon. A számítógépes adatkezelés kultúrájának, biztonságos, hatékony módszereinek kialakulásához új ismeretek, készségek elsajátítására van szükség.

Az egészségügy intézményeiben kezelt különleges adatok fokozott védelmet igényelnek, amit az informatikai rendszerek általában jelszó alkalmazásával oldanak meg. Az ellátást végző dolgozók általában több különböző informatikai rendszert használnak. Ugyanazt a jelszót nem célszerű több alkalmazáshoz használni, ezért jellemzően több jelszót kell megjegyezniük. Ehhez használhatnak különféle memoritereket és klaviatúralogikákat [1], de félő, hogy összekeverik ezeket.

Több jelszó használatához, kezeléséhez jobb megoldás lehet egy jelszómenedzser szoftver alkalmazása.

Mire használható egy jelszómenedzser?

A jelszavak mindennapi használata során hajlamosak vagyunk elfeledkezni róla, hogy digitális életünk legfontosabb és legértékesebb szereplői jelszavaink. Ha egy fájl elvész, segít a biztonsági másolat vagy a visszaállítás, ha a Windows tönkremegy, újrainstallálhatjuk, ha egy szoftver tönkremegy, újratelepíthetjük. Viszont, ha egy fontos jelszót elfelejtünk, esetleg ellopják, akkor elég nagy baj lehet.

Van persze kézenfekvőnek tűnő megoldás: fel kell írni a jelszavakat egy biztonságos, jól őrzött helyre. Legjobb talán egy tűzbiztos páncélszekrényben tárolni a jelszavak listáját, hogy senki ne láthassa, és ne tudja ellopni sem őket. Ez a megoldás a biztonságos őrzésre kiváló, de hogyan használjuk a széfbe zárt jelszavakat?

Erre a problémára ad jól alkalmazható megoldást a jelszómenedzser szoftver. A biztonságos tárolást, ugyanakkor a hatékony és kényelmes használatot is lehetővé teszi.

Egy ilyen rendszer erősen védett adatbázisban, úgynevezett széffájlban tárolja az egyes alkalmazásokhoz tartozó felhasználónév–jelszó párokat, és biztonságos kényelmi szolgáltatásokat nyújt a jelszóval védett rendszerekbe történő bejelentkezéshez.

A nagyon erős titkosítással védett széfadatbázist master jelszó védi, ami kiegészíthető kétfázisú felhasználóazonosítással is [1], ami által a biztonság jelentős mértékben növelhető.

A jelszómenedzser szoftverek erőssége, hogy nagyon biztonságos, szinte tökéletes jelszavakat generálnak, és a felhasználónév–jelszó párok adatbázisát szinkronizálják különféle eszközökre, így bármilyen környezetben alkalmazhatók.

Komoly hátrányuk viszont, hogy a master jelszó elvesztése vagy bármilyen kompromittálódása esetén a tárolt jelszavakhoz kapcsolódó összes alkalmazás rendelkezésre állása veszélybe kerülhet.

Jelszómenedzserek biztonsága

Nagyon körültekintően kell kiválasztani a jelszómenedzsert, mert sok – akár fizetős – szoftver található az interneten, aminek eredete bizonytalan, ezért használata jelentős biztonsági kockázattal jár. Elsősorban ismert forráskódú, szabad szoftvereket célszerű választani, amik általában ingyenesek is.

Egy biztonsággal kapcsolatos szoftver minőségét elsősorban a nyilvánosság garantálhatja. Ha a működést meghatározó forráskód ismert, akkor a biztonsági szakembereknek módjuk van a szoftver alapos elemzésére, támadási módszerek kipróbálására és ezzel a korrekt, biztonságos működés minőségének meghatározására. Jelentős tudományos eredménynek számít egy-egy népszerű, sok millió felhasználó által alkalmazott informatikai rendszer biztonsági réseinek feltárása. A szakmai nyilvánosság és a felhasználók nagy száma gyakorlati garanciát jelenthet egy jelszómenedzser szoftver biztonságos működésére.

A fizetős szoftverek esetében szokásos megoldások nem erősítik a bizalmat, a forráskód és a működés részleteinek ismerete nélkül a szakmai nyilvánosság erősen korlátozott, ezért az értékítélet nem lehet kellően megalapozott.

Igen tanulságos, ahogyan különféle médiumok rangsorolják és minősítik mindenféle szakmainak tűnő szempontok szerint a jelszómenedzser szoftvereket, miközben a biztonsági szakemberektől származó, tudományos igényű elemzéseket gyakran figyelmen kívül hagyják.

Például a Ziff Davis vállalat [2] által működtetett sok millió olvasóval rendelkező PC Magazine Digital Edition [3] kiadott egy elemzést és rangsort a 2016. év legjobb fizetős [4] és ingyenes [5] jelszómenedzser szoftvereiről. Mindkét kategóriában – mivel van fizetős és ingyenes változata is – a legjobbnak a LastPass [6] nevű webalapú, böngészőben futó rendszert rangsorolták. Már 2011-ben több mint egymillió felhasználója volt ennek a kényelmes, népszerű rendszernek, és azóta ez a szám még lényegesen növekedett.

A patinás University of California egyetem kutatói egy tudományos igényű cikkben [7] a LastPass 2013-as változatában kritikus sebezhetőségi hibákat találtak, ami erősen megkérdőjelezi a biztonságos használatot.

A [7] közlemény a további négy vizsgált (RoboForm [8], My 1login [9], PasswordBox [10], NeedMyPassword [11]) webalapú rendszerben is kritikus biztonsági hibákat talált, ami kétségessé teszi a webalapú technológia létjogosultságát ezen a területen.

2013 óta vajon mi változott?

Továbbra is rengeteg jelszómenedzsert lehet találni az interneten, továbbra is elemeznek és rangsorolnak a különféle médiumok, továbbra is csaknem ismeretlenek a felhasználók nagy tömegei számára a szakértő kutatók tudományos igényű biztonsági elemzései.

Joggal merül fel a kérdés: Vajon mennyire lehet ma biztonságos a sok millió felhasználó által kedvelt webalapú, de nem nyílt forráskódú, fizetős LastPass 4.0 Premium szoftver?

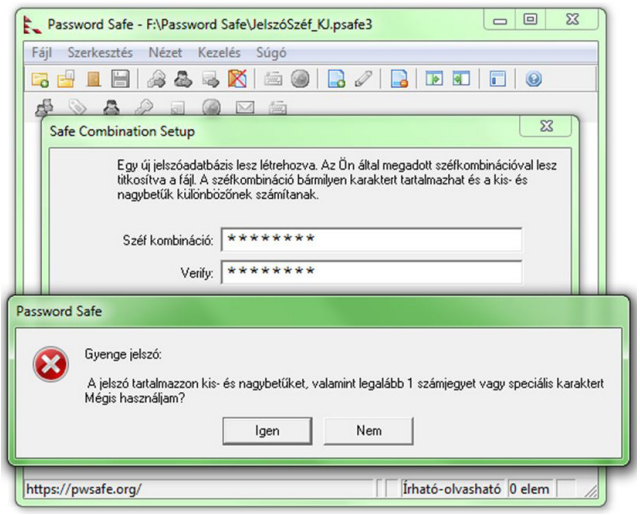
Erre a kérdésre nehéz korrekt választ adni, de a biztonsági szakemberek továbbra is az önálló alkalmazásként működő, nyílt forráskódú, szabad szoftvereket ajánlják. Ilyen például a Password Safe [12] szoftver, ami magyar nyelven is rendelkezésre áll, és *Bruce Schneier* [13], világhírű biztonsági szakember tervezte.

Jelszómenedzserek jelszavakat tartalmazó adatbázisának, széffájljának biztonságát tudományos igénnyel elemezte a University of California egyetem két kutatója a [14] közleményben. A vizsgált rendszerek közül a Password Safe adatbázis megoldása az egyetlen, ami teljesen biztonságosnak tekinthető, ellenállt a támadási próbálkozásoknak.

Elegendően biztonságosnak tekinthető a KeePass 2.x [15] szoftver is. A [14] cikk szerint elfogadhatóan biztonságos a jelszavakat tároló adatbázisa. Ez is nyílt forráskódú, ingyenes szabad szoftver, megfelel a szakmai nyilvánosság elvárásainak, ez idáig nem találtak benne kritikus mértékű sebezhetőséget. Magyar nyelvű kezelőfelülettel is rendelkezik, könnyen és kényelmesen használható.

A Password Safe jelszómenedzser

A 2002 óta fejlesztett szoftvert több millióan használják, különféle rangos díjakat is nyert. A forráskód a GitHub [15] nevű projekt hosting rendszerben található, bárki – bejelentkezés nélkül is – megnézheti. Használhatósá-



1. ábra | Gyenge jelszó megadására figyelmeztet a rendszer

gát tekintve – konkurenseihez hasonlóan – minden fontos biztonsági és kényelmi funkciót megvalósít, így egészségügyi alkalmazáshoz ajánlható. Windows, Mac OS, iOS és Android operációs rendszereken működik, ami általában megfelel az egészségügy elvárásainak is.

A rendszer nagyrészt magyar nyelvű, de a helyzetérzékeny súgó csak angol nyelven áll rendelkezésre. Nézzük most meg a jelszómenedzser-alkalmazás legfontosabb funkcióit!

Új széfadatbázis létrehozása

Első lépésként létre kell hozni egy adatbázist az érzékeny adatok biztonságos tárolásához. A széfadatbázis egy speciális, titkosított fájl lesz, amihez egy egyedi master jelszót kell rendelni, amit a rendszer találóan széfkombinációnak nevez.

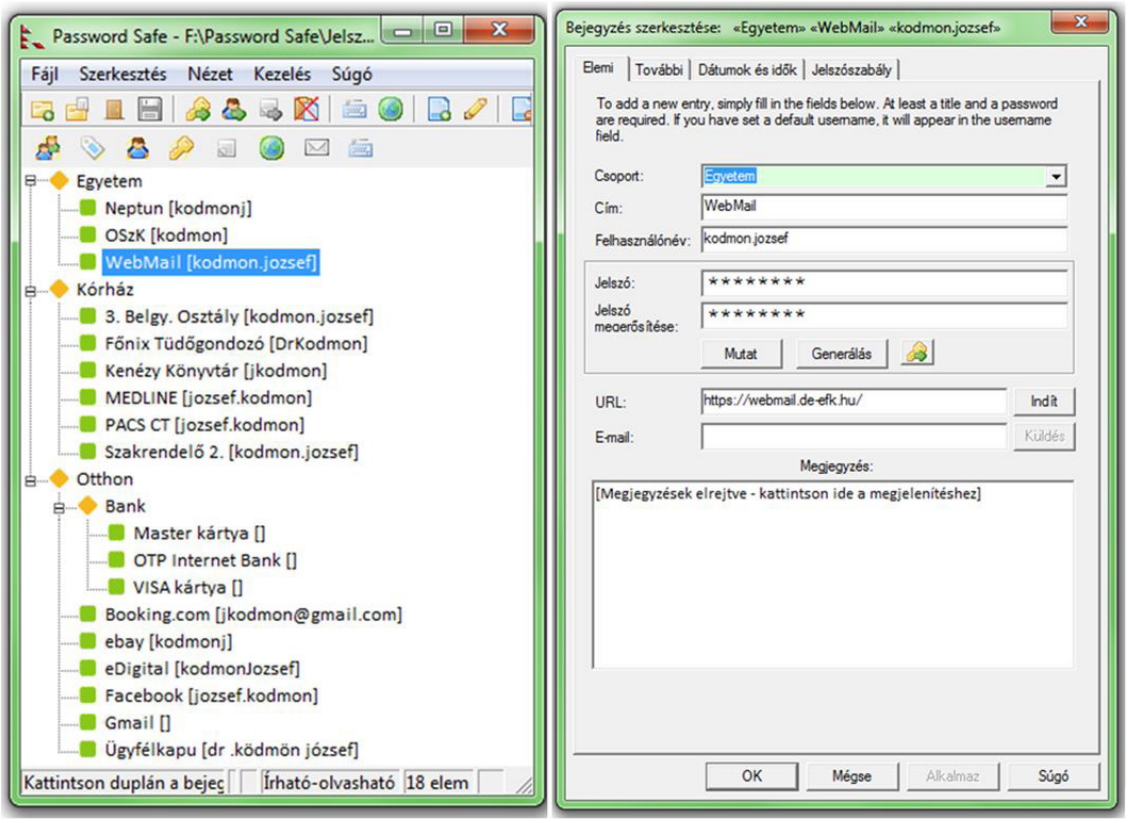
A biztonságos működés szempontjából döntő fontosságú a megfelelő master jelszó megadása, ezért igen lényeges, hogy tartalmazzon kis- és nagybetűt, számot, továbbá egyéb, billentyűzeten megtalálható jelet, a hosszának pedig legalább 10 karakternek kell lennie. Ha a master jelszó nem elég biztonságos, figyelmeztetést kap a felhasználó *(1. ábra)*.

A választott master jelszót még egyszer meg kell adni a Verify mezőben. Egyezés esetén lesz hozzárendelve a széffájlhoz.

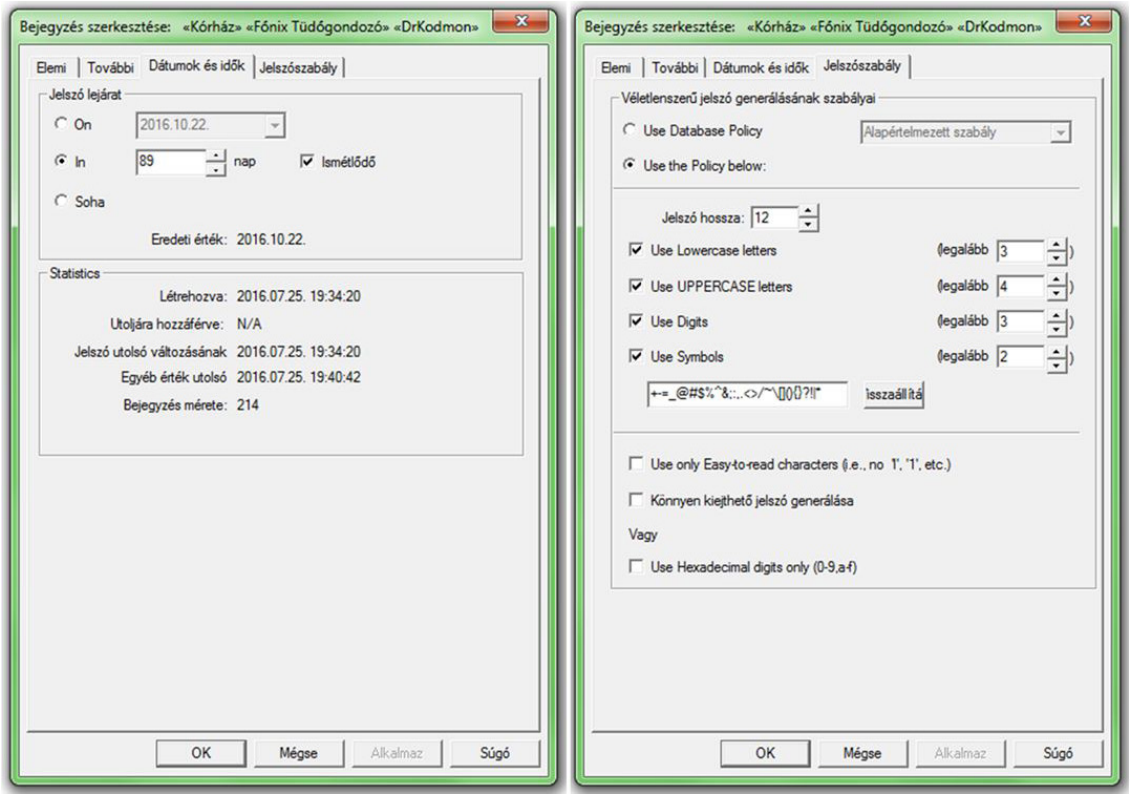
A master jelszó semmilyen módon nem állítható vissza, ezért azt nagyon körültekintően kell megválasztani és kezelni, célszerű használni az [1] cikkben leírt memoriter és billentyűzetlogika módszereket.

Bejegyzés hozzáadása

A széfadatbázisban fastruktúrába szervezetten tudjuk beírni az egyes rendszerekbe történő belépéshez szükséges adatokat. Ilyen többszintű faszerkezet látható a *2. ábra bal oldalán*.



2. ábra | Új bejegyzés hozzáadása a faszerkezetben tárolt széfadatokhoz



3. ábra | A jelszó tulajdonságainak beállítása

Minden bejegyzésnél meg kell adni legalább a bejegyzés nevét, a hozzá tartozó jelszót, és ki kell választani azt is, hogy a struktúra melyik csoportjába tartozzon *(2. ábra jobb oldala)*.

A jelszót generálni is lehet jelszószabály szerint. Az alapértelmezett szabály: három kisbetű, négy nagybetű, három szám és két egyéb jel. Így az alapértelmezett jelszó 12 karakter hosszú lesz. Ez a beállítás a jelenlegi technikai fejlettség és jelszófeltörési tapasztalatok szerint megfelel az elvárhatóan magas biztonsági követelményeknek. Az automatikus generálás kifinomult algoritmusa biztosítja, hogy az előállított jelszó nem tartalmaz olyan gyengeségeket, ami megkönnyíti a feltörést.

Az alapértelmezett jelszószabályt módosítani lehet a *3. ábra jobb oldalán* látható ablakban. Megadható az is, hogy milyen jelkészletből kerüljenek kiválasztásra az automatikusan generált jelszó karakterei. A sokrétű generálási mód biztosítja, hogy nagyon erős, szinte tökéletes jelszavakat állítsunk elő. Természetesen az is beállítható, hogy egy jelszó meddig legyen érvényben. A beállítás elvégezhető a *3. ábra bal oldalán* látható ablakban, ahol a jelszó használatával kapcsolatos statisztikai adatokat is megismerhetünk.

Mivel az automatikusan generált jelszavainkat nem kell megjegyeznünk, használhatunk lényegesen hosszabb és ezáltal biztonságosabb jelszavakat is.

A bejegyzésekben tárolt adatok segítségével történik az egyes jelszóvédett alkalmazások indításánál a bejelentkezés. Lehetőség van kézi és automatikus bejelentkezésre is.

Új jelszó megadásakor vagy jelszó cseréje esetén csak a kézi megadás jöhet szóba. A CTRL + U billentyűkombináció vágólapra másolja az aktuális bejegyzésben tárolt felhasználónevet, a CTRL + C pedig a jelszót. A vágólapról a CTRL + V kombinációval másolhatunk a megfelelő mezőbe.

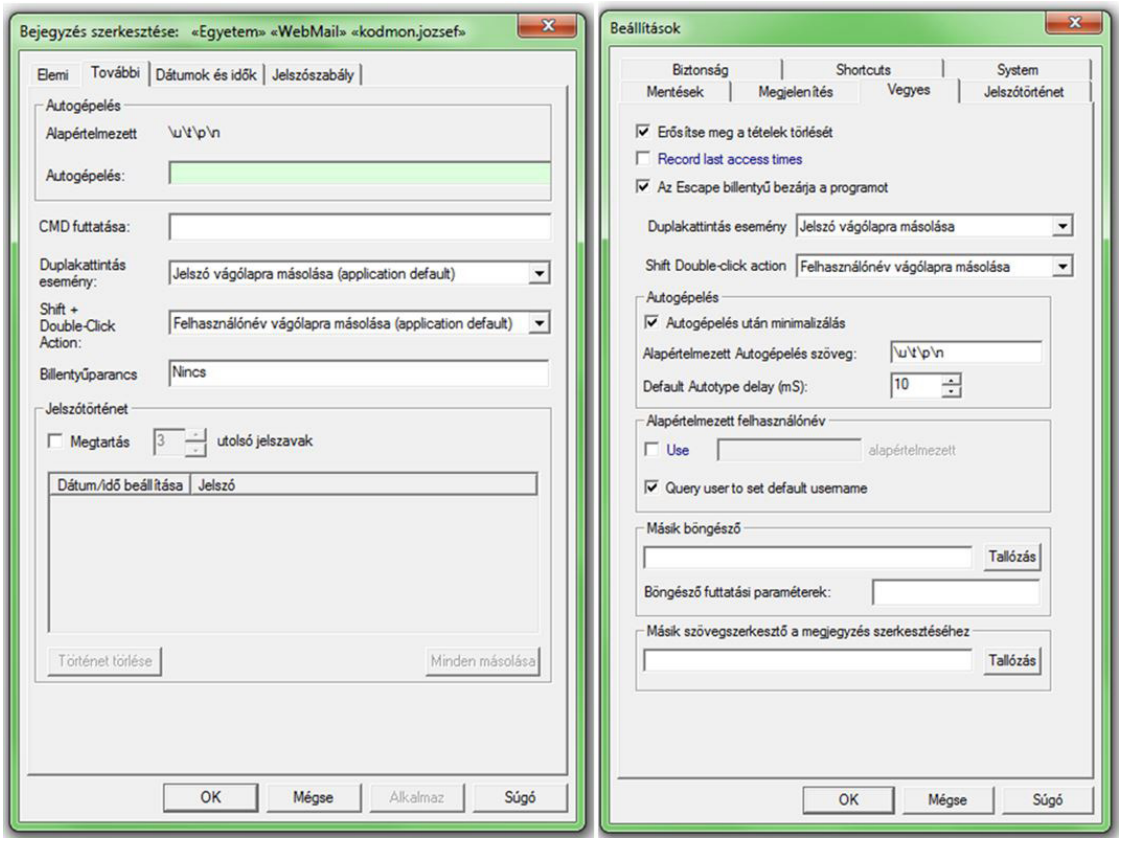
Automatikus bejelentkezés

Ha egy biztonsággal kapcsolatos rendszer használata nehézkes, olyan tevékenységeket tartalmaz, amit nem szívesen csinálunk, akkor legfeljebb csak kényszerből fogjuk használni, és nem fog mindennapi rutinná válni az alkalmazása.

Ha egy jelszómenedzser nem támogatja a könnyű és gyors bejelentkezést, nem lehet igazán sikeres.

A Password Safe igen sokrétűen beállítható automatikus bejelentkezés funkcióval rendelkezik. A használat alapfeltétele, hogy a bejegyzés létrehozásakor *(2. ábra jobb oldali ablaka)* megadjuk a használni kívánt internetes szolgáltatás bejelentkezési képernyőjének webcímét (URL), továbbá megadjuk az automatikus gépelés (Autogépelés) beállításait *(4. ábra)*.

A legfontosabb az Autogépelés sablonjának helyes megadása. Ez alapértelmezetten „\u\t\p\n”, ami a leggyakoribb folyamatot írja le: felhasználónév-megadás (\u), TAB billentyű lenyomás (\t), jelszóbeírás (\p),



4. ábra | Az automatikus gépelés beállításai

ENTER billentyű lenyomása (\n). Ha ettől eltér a bejelentkezési folyamat, akkor sokféle sablonparancs alkalmazásával hozhatjuk azt létre az Autogépelés mezőbe történő beírással *(4. ábra bal oldali ablak)*.

Ha a Kezelés/Beállítások részben megadjuk, hogy a Password Safe az operációs rendszer indulásakor automatikusan induljon el és legyen mindig látható, továbbá a bejegyzések faszerkezete induláskor legyen teljesen kibontva, akkor nagyon gyorsan és kényelmesen tudjuk használni az automatikus bejelentkezést.

Mindössze három lépésre van szükség: master jelszó megadása, kattintás a fastruktúra megfelelő bejegyzésére és végül ALT + L billentyűkombináció leütése. Ennek hatására elindul az alapértelmezett böngésző, abban pedig megjelenik a kiválasztott alkalmazás bejelentkezési képernyője, automatikusan beíródnak a bejegyzésben tárolt bejelentkezési adatok és végül megnyomódik az ENTER.

Jelszóval védett nem webes alkalmazások automatikus indításához a CMD futtatása mezőbe *(4. ábra bal oldali ablak)* kell beírni az indításhoz szükséges parancsot, és az Autogépelés mezőben kell megadni a belépés sablonját. Ekkor az előbbi három lépésben automatikusan indítható minden számítógépre installált lokális alkalmazás is.

Ilyen módon a Password Safe az összes jelszóval védett alkalmazás egyfajta indító központjává válik, meggyorsítja és nagyon biztonságossá teszi a bejelentkezéshez kötött alkalmazások használatát.

Az automatikus gépelés funkció segítségével megoldható a legegyszerűbb, két részből álló bejelentkezési eljárásnál lényegesen összetettebb belépési adatkombináció megadása is. Ilyen esetben használható a bejegyzés megadás többsoros Megjegyzés mezője *(2. ábra jobb oldali ablak)*. A megjegyzésbe írt sorokra lehet hivatkozni sablonparanccsal, és így egészen bonyolult azonosítási folyamat sablonja is megszerkeszthető, alkalmazható.

Lehetőség van például elektronikus banki rendszerekben történő azonosítóadatok vagy webáruházakban történő vásárlásnál a fizetési adatok megadására is, ahol általában több részből álló bankkártyaadatokat vagy számlaszámot is meg kell adni.

A Password Safe kényelmesnek tekinthető, mivel használatával egy tipikus webalapú alkalmazás indítása körülbelül ugyanannyi lépést igényel, mint a jelszómenedzser nélküli indítás *(1. táblázat)*.

Lényegében ugyanez a helyzet egy nem webalapú, helyi alkalmazás indítása esetén is.

A kényelmes használat mellett a Password Safe egy igen fontos előnye, hogy automatikusan generált, nagyon erős jelszavak védik alkalmazásaink biztonságát. Ne feledkezzünk meg azonban egy lényeges hátrányáról sem: a master jelszó bármilyen kompromittálódása esetén alkalmazásaink biztonságát komoly veszély fenyegetheti.

1. táblázat | Alkalmazás indítása lépéseinek összehasonlítása

Jelszóval védett webes alkalmazás indítása	
Password Safe nélkül	Password Safe használatával
Böngésző indítása – egy kattintás	Password Safe indítása – egy kattintás
Alkalmazás indítása – egy kattintás	Master jelszó megadása
Felhasználónév beírása	Bejegyzés kiválasztása – egy kattintás
Jelszó megadása	ALT + L leütése

A Password Safe biztonságos használata

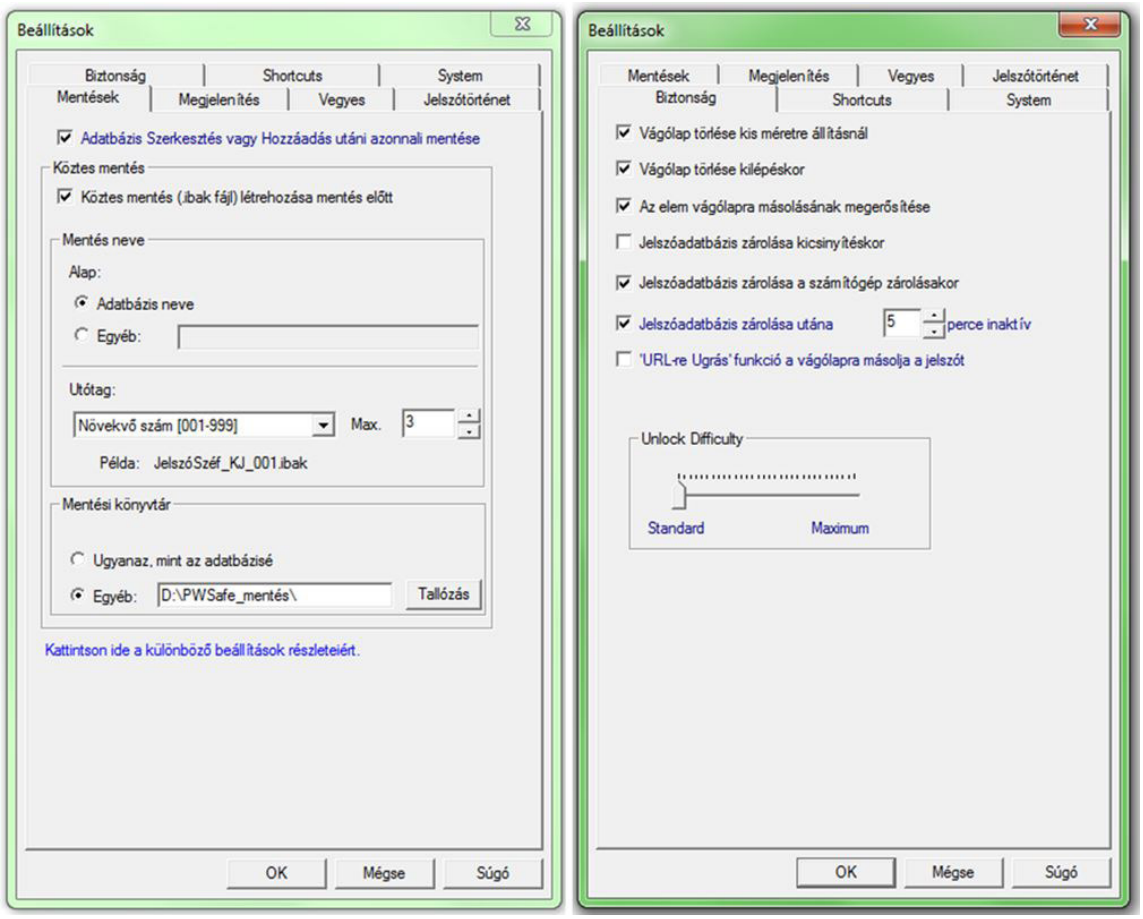
A legfontosabb biztonsági elem a master jelszó, amelynek legalább 10 karakter hosszúnak kell lennie és tartalmaznia kell kis- és nagybetűt, számot, valamint egyéb jelet. Ennek a jelszónak megjegyezhetőnek kell lennie, felidézéséhez az [1] cikkben leírt módszert érdemes követni.

A használt memoriter lehet például a következő Petőfi Sándor-versrészlet: *„Még nyílnak a völgyben a kerti virágok / Még zöldell…”* Ezt használva a master jelszó pedig lehet: *„MnavakvMz357+%=*”.

A [16], [17] és [18] közlemények szerint a jelszó rendszeres cseréje kevésbé fontos, inkább az lényeges, hogy amikor esetleg kompromittálódik, *azonnal* megváltoztassuk, hogy a támadó kevésbé tudjon visszaélni vele. Az idézett kutatások szerint tehát a gyakori jelszócsere nem éri meg, nem növeli érdemben a biztonságot, sőt inkább gyengíti azt, hiszen kényelmetlen újabb és újabb erős jelszót keresni. Az erőltetett cserének előbb-utóbb gyenge jelszó lehet az eredménye, ez pedig biztonsági kockázatot rejthet magában. A jelszócsere nem igazán kényelmesen valósítható meg a Password Safe rendszerben sem, így a gyakori váltás ebben az esetben sem ajánlott.

Így tehát a master jelszót és a bejegyzésekben szereplő alkalmazások jelszavait nem kell gyakran cserélni, elengedő évente egy-két alkalommal.

Érdemes viszont legalább havonta ellenőrizni a [19] honlapon, hogy bejelentkezési adataink nem kompromittálódtak-e. E-mail-címünk vagy bejelentkezésnél használt felhasználónevünk megadása után az alkalmazás ellenőrzi a feltört rendszerek aktuális adatbázisai alapján, hogy biztonságosak-e bejelentkezési adataink. Ez az adatbázis kizárólag az ismertté vált feltörési eseteket tartalmazza, ezért érdemes figyelni minden gyanús, kompromittálódásra utaló jelre. A legfontosabb pedig, hogy



5. ábra | Mentési és biztonsági beállítások

erős jelszavakat használjunk, azok feltörése nagyon időigényes, a támadók jellemzően kihagyják, nem erőltetik az ilyen jelszó megszerzését. Jobban szeretik a gyorsan feltörhető, gyenge jelszavakat, abból is akad bőven, ahogyan az a [19] honlapon látható.

A jelszótulajdonos esetleges cselekvőképtelenné válása esetén, továbbá bármilyen más katasztrófahelyzet bekövetkezésénél gondoskodni kell a master jelszó elérhetőségéről. Az aktuálisan használatban lévő jelszót fel kell jegyezni és zárt borítékban megfelelően védett helyen kell tárolni. A tárolási módszereknek követniük kell a munkahely szabályait, illetve az otthoni értéktárolási szokásokat. Nagyon sok – bár ritkán jelentkező – probléma kerülhető el ezzel az eljárással, ezért hajlamosak vagyunk megfeledkezni róla. Minden hagyományos értéket általában megfelelően kezelünk és védünk, vonatkozzon ez a jelszóra is, mint digitális életünk legnagyobb értékére.

Eldöntendő az is, hogy egy vagy több széfet akarunk-e használni. Tipikusan a munkahelyi és otthoni alkalmazásokat szokás szétválasztani. Ez azonban nem életszerű és nem is kényelmes, hiszen gyakran előfordulhat, hogy otthoni alkalmazást szeretnénk a munkahelyünkön használni és megfordítva, ami az egyszéfes megoldást favorizálja.

A Password Safe alkalmas kétfázisú felhasználóazonosításra [1] is. A legjobban a Yubico Inc. [20] által gyártott YubiKey tokennel tud együttműködni.

Egyszerűbb és olcsóbb lehetőség, ha a Password Safe szoftvert hordozható (portable) módon installáljuk egy pendrive-ra vagy SD-kártyára. A teljes rendszer kevés helyet foglal, elegendő körülbelül 12 MB. A szoftveren és a széfen kívül más fájlokat nem célszerű velük együtt tárolni, hiszen a pendrive-ot, illetve SD-kártyát most tokenként használjuk.

Nagy felhasználói rugalmasságot adhat a széffájl felhőben történő tárolása. Ez lehetővé teszi a széf elérését különféle eszközökről, de nem jelent lényeges biztonsági kockázatot, hiszen a széffájl erős titkosítással védett. Célszerű automatikus szinkronizálással rendelkező felhőszolgáltatást választani, mert így mindig az aktuális széfváltozat lesz elérhető.

Nagyon ajánlott biztonsági másolatot készíteni a széffájlról úgy, hogy a másolat fizikailag más helyen legyen tárolva, mint a használatban lévő. Legjobb egy olyan pendrive, amit nem használunk tokenként. A másolatkészítés beállításainak részletei láthatók az *5. ábra bal oldali ablakában*. A biztonsági beállítások részletei pedig az *5. ábra jobb oldali ablakában* láthatók. Az Unlock Difficulty csúszka a széffájl titkosításának erősségét állítja. A Standard beállítás teljesen megfelel egy egészségügyben dolgozó felhasználó biztonsági igényének. Nagyobb érték beállítása lassíthatja a széf megnyitását, mivel a titkosítás feloldása erősen processzorigényes művelet.

Ha nem akarunk módosításokat a bejegyzésekben vagy a beállításokban, csupán alkalmazásokat indítunk a Password Safe rendszerből, elegendő a széfadatbázist csak olvasásra megnyitni. Ezt beállíthatjuk a master jelszó megadásakor, a megfelelő jelölőnégyzetbe kattintva.

Az egészségügyi alkalmazás sajátosságai

Az egészségügyben alkalmazott informatikai rendszerek biztonsága nagyrészt a jelszavak erősségétől függ. A legtöbb biztonsági incidens a nem megfelelően megválasztott vagy felelőtlenül használt jelszavakra vezethető vissza.

Az egészségügyi környezet nem tolerálja a bonyolult és gyakran költséges adatvédelmi, biztonsági megoldásokat. A gyógyítással, betegellátással foglalkozó munkatársak nem fogják használni a nagyon biztonságosnak tartott, de munkájukat lassító, nehezítő vagy bármilyen szempontból körülményessé tévő megoldásokat. Az ilyen rendszerek használatának kikényszerítésével többnyire nem érhető el az informatikai biztonság növekedése. Sőt az ellenérzésből fakadó fegyelmezetlen magatartás nagy biztonsági kockázatot jelenthet.

Egy jelszómenedzser szoftver használata nem nehezíti vagy lassítja a bejelentkezési folyamatot, így életszerű egy ilyen megoldás általános bevezetése.

Az egészségügyben dolgozó rendszergazdák, informatikusok és felső vezetők számára kimondottan ajánlott jelszómenedzser használata kétfázisú azonosítással. Tokenként megfelel egy USB-portra csatlakoztatott kis kapacitású pendrive is. Ezek ára már elfogadhatóan alacsony, a szűkös egészségügyi költségvetés is elbírja ezt a beruházási terhet. A többi, informatikát alkalmazó felhasználónak elegendő biztonságot ad a token nélküli jelszómenedzser használata.

Egészségügyi alkalmazásra elsősorban a Password Safe szoftver ajánlható. Teljes mértékben megfelel a legmagasabb szintű biztonsági elvárásoknak, könnyen kezelhető magyar nyelven is, az automatikus gépelés által nagyon kényelmesen használható és nem lassítja vagy nehezíti a bejelentkezési folyamatot.

Alternatívaként elfogadható a KeePass 2.x [21] egészségügyi alkalmazása is. Megfelelően biztonságos és van magyar nyelvű kezelőfelülete is. Az automatikus gépelés funkció hasonlóan kényelmes használatot biztosít, mint a Password Safe esetében.

Mivel az egészségügyi alkalmazásokban tipikusan csak jelszó védi az érzékeny adatokat, egy jelszómenedzser alkalmazásától a biztonság szignifikáns növekedése várható, ami meghatározó fontosságú egészségügyi informatikai elvárás.

Anyagi támogatás: A közlemény megírása anyagi támogatásban nem részesült.

A cikk végleges változatát a szerző elolvasta és jóváhagyta.

Érdekeltségek: A szerzőnek nincsenek érdekeltségei.

Irodalom

[1] *Ködmön, J., Csajbók Z. E.:* Information security in health care. [Információbiztonság az egészségügyben.] Orv. Hetil., 2015, *156*(27), 1075–1080. [Hungarian]
[2] https://www.ziffdavis.com
[3] http://www.pcmag.com
[4] *Rubenking, N. J.:* The Best Password Managers of 2016. July 7, 2016. http://www.pcmag.com/article2/ 0,2817, 2407168,00.asp
[5] *Rubenking, N. J.:* The Best Free Password Managers of 2016. July 7, 2016. http://www.pcmag.com/article2/ 0,2817, 2475964,00.asp
[6] https://lastpass.com
[7] *Li, Z., He, W., Akhawe, D., et al.:* The Emperor's new password manager: Security analysis of web-based password managers. In: Proceedings of the 23rd USENIX Security Symposium, August 20–22, 2014, San Diego, CA. USENIX Association, 2014, 465–479.
[8] http://www.roboform.com
[9] https://www.my1login.com
[10] https://www.passwordbox.com
[11] https://www.needmypassword.com
[12] https://pwsafe.org
[13] https://www.schneier.com
[14] *Gasti, P., Rasmussen, K. B.:* On the security of password manager database formats. In: Computer Security – ESORICS 2012. Lecture Notes in Computer Science, Vol. 7459, 770–787. Springer, Heidelberg, 2012.
[15] https://github.com
[16] *Schneier, B.:* Changing Passwords. https://www.schneier.com/blog/archives/2010/11/changing_passwo.html
[17] *Herley, C.:* So long, and no thanks for the externalities: the rational rejection of security advice by users. http://research.microsoft.com/en-s/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf
[18] *Zhang, Y., Monrose, F., Reiter, M. K.:* The security of modern password expiration: An algorithmic framework and empirical analysis. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, October 4–8, 2010, Chicago, Illinois, USA. ACM, New York, 2010, 176–186.
[19] https://haveibeenpwned.com
[20] https://www.yubico.com
[21] http://keepass.info

(Ködmön József dr.,
Nyíregyháza, Géza utca 47. fszt. 8., 4400
e-mail: jkodmon@gmail.com)